

# Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 31.10.2026

---

## Vertragsparteien

**Verantwortlicher (Auftraggeber):** der Kunde von IDO Ticket, wie in seinem Konto angegeben (im Folgenden „Kunde“)

**Auftragsverarbeiter (Auftragnehmer):** IDO GmbH, Anderslebener Straße 40, 39387 Oschersleben, vertreten durch den Geschäftsführer Martin Leue, E-Mail [info@idoticket.de](mailto:info@idoticket.de) (im Folgenden „wir“)

Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen von IDO Ticket (§ 8 AGB) und gilt für jedes Konto, ohne dass er gesondert unterschrieben werden muss. Er wird in elektronischer Form geschlossen (Art. 28 Abs. 9 DSGVO). Die aktuelle Fassung steht unter <https://idoticket.de/avv>.

## § 1 Gegenstand und Dauer

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch uns im Auftrag des Kunden, wenn er IDO Ticket (idoticket.de) nutzt, um Anfragen seiner eigenen Kunden („Endkunden“) zu bearbeiten. Den Umfang der Leistungen beschreiben die AGB und die Preisseite. Dazu gehören:

- das Entgegennehmen von Tickets, Nachrichten und Anhängen aus den Anwendungen des Kunden über die Programmierschnittstelle (API),
- die Speicherung von Tickets, Nachrichten, internen Notizen, Anhängen und Endkunden-Daten und ihre Anzeige im Helpdesk,
- der Versand von Benachrichtigungen per E-Mail an Endkunden und an Mitarbeiter des Kunden sowie das Entgegennehmen von Antworten per E-Mail und ihre Zuordnung zum Ticket,
- die Bereitstellung der Tickets eines Endkunden an die jeweilige Anwendung des Kunden über die API.

(2) Nicht Gegenstand dieses Vertrags sind Daten, die wir als eigener Verantwortlicher verarbeiten, zum Beispiel die Zugangs- und Abrechnungsdaten des Kontos, Server-Protokolle, die Reichweitenmessung und Anfragen über unser Kontaktformular. Dafür gilt unsere Datenschutzerklärung.

(3) Der Vertrag gilt, solange das Konto besteht, und darüber hinaus, solange wir nach Ende des Abos noch Daten des Kunden speichern (§ 9). Pflichten, die ihrer Natur nach über das Vertragsende hinaus gelten, insbesondere zur Löschung und zur Vertraulichkeit, bleiben bestehen.

## § 2 Art und Zweck der Verarbeitung, Art der Daten, betroffene Personen

(1) **Art der Verarbeitung:** Erheben (über die API und per E-Mail), Speichern, Anzeigen, Übermitteln an die Anwendungen des Kunden, Versenden von E-Mails, Protokollieren und Löschen.

(2) **Zweck:** Bearbeitung von Support-Anfragen der Endkunden des Kunden und Kommunikation mit ihnen.

(3) **Art der Daten:**

- Endkunden-Daten: Kundennummer in der Anwendung des Kunden, Name, E-Mail-Adresse, Firma,
- Inhalte der Tickets: Betreff, Text, Kategorie, Priorität, Status und vom Kunden frei gewählte Kontextangaben (etwa Seite, Tarif, Version, Browser),

- Anhänge wie Screenshots, Bildschirmvideos und Dokumente mit allen darin enthaltenen Angaben; je nach Inhalt auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, soweit Endkunden sie mitteilen,
- E-Mails von Endkunden an das Antwortpostfach mit Kopfzeilen und Anhängen,
- Daten der Mitarbeiter des Kunden: Name, E-Mail-Adresse, Zuständigkeiten, Verlauf ihrer Antworten und Notizen.

(4) **Betroffene Personen:** Endkunden und deren Ansprechpartner, weitere Personen, die in Tickets oder Anhängen genannt oder zu sehen sind, sowie Mitarbeiter des Kunden.

### § 3 Weisungen

(1) Wir verarbeiten die Daten nur auf dokumentierte Weisung des Kunden. Die Weisungen ergeben sich aus diesem Vertrag und aus der Nutzung der Funktionen von IDO Ticket: Was der Kunde im Helpdesk oder über die API anlegt, ändert, beantwortet, einstellt oder löscht, gilt als Weisung. Weitere Weisungen erteilt der Kunde in Textform, etwa per E-Mail an [info@idoticket.de](mailto:info@idoticket.de). Weisungsberechtigt ist, wer einen Zugang mit allen Rechten hat oder den Kunden vertritt.

(2) Verpflichtet uns das Recht der EU oder Deutschlands zu einer anderen Verarbeitung, teilen wir dem Kunden das vorher mit, sofern das Recht diese Mitteilung nicht verbietet (Art. 28 Abs. 3 lit. a DSGVO).

(3) Halten wir eine Weisung für rechtswidrig, weisen wir den Kunden unverzüglich darauf hin (Art. 28 Abs. 3 Satz 3 DSGVO).

### § 4 Unsere Pflichten

(1) Wir verarbeiten die Daten ausschließlich, um die vereinbarten Leistungen zu erbringen, nicht für eigene Zwecke, nicht für Werbung und nicht zum Training von KI-Modellen. Inhalte der Tickets sehen wir uns nicht an; ist das ausnahmsweise zur Behebung eines Fehlers nötig, nur auf Anfrage oder mit Zustimmung des Kunden.

(2) Personen, die bei uns Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht (Art. 28 Abs. 3 lit. b DSGVO).

(3) Wir treffen die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 1 beschrieben sind. Wir dürfen sie an den Stand der Technik anpassen, solange das Schutzniveau nicht sinkt.

(4) Wir unterstützen den Kunden mit geeigneten Maßnahmen dabei, Anfragen betroffener Personen zu beantworten (Art. 12 bis 23 DSGVO). Wenden sich Betroffene direkt an uns, leiten wir die Anfrage unverzüglich an den Kunden weiter.

(5) Wir unterstützen den Kunden bei seinen Pflichten aus Art. 32 bis 36 DSGVO im Rahmen der Art der Verarbeitung und der uns vorliegenden Informationen.

(6) Werden uns Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt, melden wir sie dem Kunden unverzüglich per E-Mail an die Adresse seines Kontos, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit sie uns vorliegen.

(7) Wir verarbeiten die Daten ausschließlich in Deutschland (§ 7).

## **§ 5 Pflichten des Kunden**

- (1) Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich, insbesondere für die Information seiner Endkunden über den Einsatz von IDO Ticket.
- (2) Er hält die API-Schlüssel seiner Anwendungen geheim, setzt sie nur auf seinen Servern ein und erneuert einen Schlüssel, wenn er bekannt geworden sein könnte.
- (3) Er vergibt Zugänge zum Helpdesk nur an berechnigte Personen und deaktiviert Zugänge, die nicht mehr gebraucht werden.
- (4) Er informiert uns unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

## **§ 6 Unterauftragsverarbeiter**

- (1) Der Kunde ist mit den in Anlage 2 genannten Unterauftragsverarbeitern einverstanden (allgemeine Genehmigung nach Art. 28 Abs. 2 DSGVO).
- (2) Wollen wir einen Unterauftragsverarbeiter hinzunehmen oder ersetzen, informieren wir den Kunden mindestens vier Wochen vorher per E-Mail an die Adresse seines Kontos. Der Kunde kann der Änderung bis zu ihrem Wirksamwerden in Textform widersprechen. Können wir den Einwand nicht ausräumen, kann der Kunde den Vertrag zum Wirksamwerden der Änderung kündigen.
- (3) Wir verpflichten jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO).
- (4) Kein Unterauftragsverarbeiter im Sinne dieses Vertrags ist der Zahlungsdienstleister Stripe, der nur die Daten des Abos verarbeitet und keinen Zugang zum Helpdesk hat (dafür sind wir selbst Verantwortlicher). Ebenso wenig die Mailanbieter der Endkunden, an die wir E-Mails zustellen.

## **§ 7 Ort der Verarbeitung**

Die Verarbeitung findet ausschließlich auf Servern in Rechenzentren in Deutschland statt. Eine Übermittlung in ein Drittland findet nicht statt. E-Mails an Endkunden verlassen unseren Mailserver auf dem Weg zum Mailanbieter des Endkunden, den dieser selbst gewählt hat. KI-Dienste setzen wir für die Verarbeitung der Tickets nicht ein.

## **§ 8 Nachweise und Kontrollen**

- (1) Wir weisen die Einhaltung unserer Pflichten in erster Linie durch Auskünfte und Unterlagen nach, etwa die Beschreibung der Maßnahmen in Anlage 1 und Nachweise unserer Unterauftragsverarbeiter (zum Beispiel das ISO/IEC-27001-Zertifikat der Hetzner Online GmbH für ihre Rechenzentren).
- (2) Reicht das nicht aus, kann der Kunde sich nach Anmeldung mit angemessener Frist während der üblichen Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer von der Einhaltung überzeugen (Art. 28 Abs. 3 lit. h DSGVO). Die Kontrolle darf den Betrieb nicht unverhältnismäßig stören und muss die Vertraulichkeit der Daten anderer Kunden wahren.

## **§ 9 Löschung und Rückgabe**

- (1) Auf Wunsch stellen wir dem Kunden vor dem Ende des Vertrags seine Tickets mit Nachrichten und Anhängen in einem gängigen Format (JSON mit den Dateien) bereit. Das ist die Rückgabe der Daten im Sinne von Art. 28 Abs. 3 lit. g DSGVO.

(2) Im Einzelnen gelten folgende Fristen:

| Daten                                                         | Löschung                                                                 |
|---------------------------------------------------------------|--------------------------------------------------------------------------|
| Tickets mit Nachrichten, internen Notizen und Anhängen        | solange das Konto besteht; einzelne Tickets auf Weisung des Kunden       |
| Endkunden (Kundennummer der App, Name, E-Mail-Adresse, Firma) | solange das Konto besteht; auf Weisung des Kunden mit allen Tickets      |
| Alle Daten nach Ende des Abos                                 | 30 Tage nach Abo-Ende, dann vollständig gelöscht                         |
| Alle Daten nach einer Testphase ohne Abo                      | 30 Tage nach Ende der Testphase                                          |
| Postausgang (versendete Benachrichtigungen)                   | nach 30 Tagen                                                            |
| Webhook-Zustellungen an die eigene App (Protokoll mit Inhalt) | nach 30 Tagen                                                            |
| Eingegangene Antwort-Mails im Antwortpostfach                 | sofort nach Übernahme ins Ticket; nicht zuzuordnende Mails nach 30 Tagen |

(3) Sicherungskopien werden im Rahmen ihres üblichen Zyklus überschrieben, spätestens 30 Tage nach der Löschung.

## § 10 Haftung und Schlussbestimmungen

- (1) Für die Haftung gilt Art. 82 DSGVO; im Übrigen gelten die Haftungsregeln der AGB.
- (2) Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes den AGB vor.
- (3) Es gilt deutsches Recht. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam.

## Anlage 1: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

### Vertraulichkeit

- **Rechenzentrum:** Die Server stehen in Rechenzentren der Hetzner Online GmbH in Deutschland. Zutritt und physische Sicherheit regelt Hetzner; deren Informationssicherheits-Managementsystem ist nach ISO/IEC 27001 zertifiziert (ein Zertifikat von Hetzner, nicht der IDO GmbH). Wir selbst haben keinen physischen Zugang zu den Servern.
- **Zugang zu den Servern:** nur für beauftragte Administratoren der IDO GmbH, nur über verschlüsselte Verbindungen.
- **Anmeldung im Helpdesk:** Passwort mit mindestens 10 Zeichen, gespeichert nur als Hash (bcrypt). Anmeldeversuche sind je Anschluss und je Zugang begrenzt.
- **Sitzung:** Sitzungs-Cookie nur über HTTPS, für Skripte nicht lesbar (HttpOnly), nicht an fremde Seiten mitgesendet (SameSite), ungültig nach längerer Inaktivität.
- **API-Schlüssel:** je Anwendung, nur als SHA-256-Hash gespeichert, jederzeit im Helpdesk erneuerbar; die Anwendung sieht nur Tickets ihrer eigenen Endkunden; Fehlversuche sind begrenzt.
- **Trennung:** Jede Abfrage ist an das Konto des angemeldeten Mitarbeiters oder des API-Schlüssels gebunden, Anhänge liegen in getrennten Ordnern je Konto. Mitarbeiter sehen nur die Anwendungen, die ihnen freigegeben sind.
- **Interne Notizen:** werden über die API nie ausgegeben, auch nicht ihre Anhänge.

- **Transport:** Alle Verbindungen zur Anwendung laufen über HTTPS (TLS) mit HSTS; der Mailversand nutzt TLS, soweit der empfangende Server es anbietet.

## Integrität

- **Anhänge:** Der Dateityp wird am Inhalt erkannt und gegen eine Liste erlaubter Typen geprüft; Dateien werden so ausgeliefert, dass der Browser sie nicht als Webseite ausführt (nosniff, eigene Content-Security-Policy).
- **Antworten per E-Mail:** Zuordnung zum Ticket nur über unsere eigene Mail-Kennung oder eine signierte Kennung im Betreff. Mails von anderen Absendern als dem Endkunden landen als interne Notiz, nie als Nachricht des Endkunden.
- **Verlauf:** Änderungen an Status, Priorität und Zuständigkeit werden mit Zeitpunkt und Mitarbeiter am Ticket festgehalten.
- **Schutz der Anwendung:** CSRF-Schutz für alle Formulare, strenge Content-Security-Policy, keine Skripte oder Schriften fremder Anbieter, Einbetten in fremde Seiten untersagt, Bot-Schutz ohne externen Dienst.

## Verfügbarkeit und Belastbarkeit

- Datenbank und Anhänge werden regelmäßig gesichert. Vor jeder Aktualisierung der Anwendung wird der neue Stand automatisch geprüft.
- E-Mails, die nicht sofort zugestellt werden können, werden in einer Warteschlange mehrfach erneut versucht.

## Regelmäßige Überprüfung

- Wir überprüfen die Maßnahmen bei jeder wesentlichen Änderung der Anwendung und passen sie an den Stand der Technik an. Unterauftragsverarbeiter setzen wir nur mit Vertrag zur Auftragsverarbeitung ein (Anlage 2).

## Anlage 2: Unterauftragsverarbeiter

| Unternehmen                                                                           | Leistung                                                                                                                                                                                        | Ort der Verarbeitung          |
|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| <b>Hetzner Online GmbH</b><br>Industriestr. 25, 91710<br>Gunzenhausen,<br>Deutschland | Rechenzentrum und Server: Betrieb der Anwendung, der Datenbank mit Tickets, Nachrichten und Kunden, der Ablage der Anhänge sowie des Mailservers für Benachrichtigungen und das Antwortpostfach | Deutschland<br>kein Drittland |

Stand dieser Fassung: 31.10.2026

---

Dokument erstellt am 31.10.2026 aus <https://idoticket.de/avv>. Elektronisch geschlossen als Bestandteil der AGB, ohne Unterschrift gültig (Art. 28 Abs. 9 DSGVO). IDO GmbH · Anderslebener Straße 40 · 39387 Oschersleben · Amtsgericht Stendal, HRB 106935